UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,773	12/30/2003	Willard M. Wiseman	42P17259	8213

8791 7590 12/21/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	**PAPER NUMBER**
2139	

MAIL DATE	DELIVERY MODE
12/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/748,773	WISEMAN ET AL.	
	Examiner	Art Unit	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/15/2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-28 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 6, 11 and 21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 6, 11 and 21 recite the limitation "the group" in the second line. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trusted Platform Module – White Paper hereafter TPM in view of Applied Cryptography and TCG Main Specification Version 1.1a hereafter TCG.

Regarding claims 1, 8, 13, 16, 23 and 26:

TPM discloses a method comprising:

requesting a service for a platform from a service provider [*page 15, Outlook requests a service from Verisign; examiner notes that it would have been obvious by one of ordinary skill in the art at the time of invention that the service provided by Verisign could have been any other service that was well known at the time (VPN, web, email, etc.)*];

receiving a service key request for the service from the service provider [*page 15, the figure shows Verisign uses TPM CSP to talk to TPM hardware, after which, the TPM generates a new key pair; it is inherent that Verisign sent a key request to the TPM*];

generating a public key pair and returning a public key of the key pair to the service provider [*TPM generates a new key pair and sends the public key pair to Verisign*];

certifying the use of the service for the platform [*by using the public key of the platform, one is certifying the service for the platform will be run on that platform*];

TPM discloses binding secret data to a platform [*page 13*], but does not disclose the public key (service key) being bound to one or more configurations of the platform or exchanging a session key.

TCG discloses a TPM_Seal command [*page 151*] that stores a secret key to a configuration of the platform configuration registers. It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of TPM to allow the TPM_Seal command to store the secret key to a configuration so the key can only be used when the platform is in that configuration [*TCG, page 151*]. TCG and TPM do

not disclose an exchanging of a session key. Applied Cryptography discloses a hybrid cryptosystem that is used to exchange a session key by using public key cryptography [*page 32-33*]. It would have been obvious to modify the method of TPM and TCG to allow for a session key exchange using the public key that is bound to a configuration of the platform, thus the session key would only be usable by a platform that could decrypt the session key so the service would be limited to that configuration.

Regarding claims 2-5, 9, 10 and 17-20:

TPM discloses the use of attestation identity key certificates [*page 15*]. Certificates are well known in the art to provide attestation to an identity of user/device and are often attested to by a trusted third party (Certificate Authority). It would have been obvious to allow the service provider to provide the identifying credential as it would have yielded predictable results to one of ordinary skill at the time of the invention.

Regarding claims 6, 11, 14, 21, 24 and 27:

TPM, TCG, and Applied Cryptography disclose the method of claim 1, wherein certifying the use of the service includes a process selected from the group of producing hash data relating to the one or more acceptable configurations; and confirming that a chosen configuration is included in a set of values representing the one or more acceptable configurations [*TCG page 151, it is inherent that the TPM_Seal command saves the configuration of registers; proof of the platform configuration occurs when the UNSEAL operation succeeds*].

Regarding claims 7, 12, 15, 22, 25 and 28:

TPM, TCG, and Applied Cryptography disclose the method claim 1, wherein the service key is limited to platform configuration register values that represent the one or more acceptable platform configurations [*TPM page 13, while binding secret data to the platform, the TPM merges the data together with the values contained in one or more PCR registers and then encrypts the combination as a whole. At a later time, when the secret data needs to be accessed, the values of the necessary platform configurations are calculated and the data is released for use only if the stored values match; decrypting with the sealed key is confirmation that the platform was in a given configuration*].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100